Journal of IoT in Social, Mobile, Analytics, and Cloud (ISSN: 2582-1369)
www.irojournals.com/iroismac/

Application of Federated Learning to Detect Malicious Behavior in Internet of Vehicles

Manas Kumar Yogi[1], Dwarampudi Aiswarya[2], Devisetti Sreeja[3]

[1, 2] CSE Department, [3] CSE-AI & ML Department, Pragati Engineering College (A), Surampalem, A.P, India.

E-mail: [1]manas.yogi@gmail.com, [2]aiswarya.d@pragati.ac.in, [3]sreejadevisetti@gmail.com

Abstract

With the escalating application of the Internet of Things (IoT) in several fields, implementation of IoT in the automotive ecosystem is currently one of the critical concerns due to the enormous potential for its expansion in unimaginable ways. Internet of Vehicles (IoV) applies to the present-day human-driven vehicles as well as impending autonomous ones. Smart transportation is significantly safer, cost-effective, more convenient, and more efficient. Despite offering plenty of benefits, IoV face serious issues including big data problems, user security and privacy, and vehicle reliability. Reliable connection channels are established but this doesn't eliminate the cyber risks associated with them. With the increasing frequency of these security incidents in IoV, guarding against these attacks has been the foremost priority. Regardless of the standard protocols and established frameworks, these attacks are still likely to endanger the vehicle and user privacy and security. To address the security and privacy issues, the primary focus of this paper is the application of federated learning to detect attacks on the security and privacy aspects of the IoV. Without using centralized data, the federated learning technique develops the prediction model utilizing user data from the devices. Thus, the model is collaborative and shared, and as model training comes down to devices, the user's data is secure as training data resides on the device and no specific versions are maintained in the cloud. Hence, the main objective is to employ a federated learning approach to ascertain any kind of malevolent conduct in the connected vehicle systems and propagate trusted, authentic and reliable information for better deployment.

Keywords: Internet of Vehicles (IoV), Federated Learning, Privacy, Security, Cyber attacks

1. Introduction

DOI: https://doi.org/10.36548/jismac.2023.1.002
Received: 13.01.2023, received in revised form: 13.02.2023, accepted: 01.03.2023, published: 10.03.2023

Internet of Vehicles (IoV) is the emerging technology that enables real-time communication between various entities such as vehicles, pedestrians, infrastructure, etc. by integrated multi-communication modules. It is the network of vehicles interconnected to exchange information for the benefit of enhanced performance, safety, and environment. It is established using hardware components like sensors, road lanes, etc., software components for object detection, pedestrian detection, etc., networking technologies like cloud computing, Wi-Fi, Bluetooth, etc., and other additional services including GPS, weather monitoring, etc. Communication between vehicles, devices, and other infrastructure must be established such that there is low-latency delivery. So, connecting via a cloud technology is most preferred as it is scalable and flexible, provides reliable connections between several devices, offers deployment, and makes innovation easier. Links between the surrounding environment and cellular vehicles (C-V2X) can be established through distinct modes of communication such as V2V, V2N, V2D, V2I, V2P, to name a few. Vehicle-to-Vehicle (V2V) connections help vehicles interact with each other by following a wireless protocol called Dedicated Short Range Communications (DSRC) and Global Positioning System (GPS) to avoid collisions, and share functional data [1]. The communication happens through public key infrastructure and helps in the exchange of information such as position and speed of surrounding vehicles, parking spots, changing lanes, preventing collisions, etc. Vehicle-to-Network (V2N) communications facilitate communication between different kinds of vehicles, and traffic signals and hence exchange information about traffic congestion, accidents, and receive alerts. Vehicle-to-Pedestrian (V2P) communication can be achieved through systems like vehicle devices, and Vehicle Road User protection devices which include sensors to capture the people on the road and give cautions accordingly. Vehicle-to-Infrastructure (V2I) communication can be bi-directional and wireless, and can enable typical communications between vehicles and network infrastructure like lane markings, traffic signs, etc. Infrastructure can share information about crashes, jams, etc. in an Intelligent Transportation System (ITS) [2]. The architecture of IoV can be primarily categorized into three main parts such as service platform typically cloud, media like V2X communication, and devices such as intelligent devices and connected vehicles.

Securing vehicles and devices is as important as ensuring smooth communication and functioning of IoV. Quality of Experience (QoE) is an essential part of the smart vehicle communication and information exchange as high quality data needs to be transferred/received from one vehicle to another continuously. The data transmission rate determines the end user's quality of experience and hence needs to be maintained in parallel with security measures.

Flexible and scalable connections should be in place and should meet the expectations of the users. Quality of Service (QoS) relates to technology which ensures performance of vital applications with finite network volumes [3]. It helps on optimizing the routing paths by making decisions depending upon the position of the vehicles, network topology, etc. Ensuring both the QoE/QoS and privacy is quite a challenging task and needs to be tackled to ensure the smart transportation is in effect and reliable. To enhance security in ITS, buffer-aware QoE/QoS came into picture by compromising the quality. To amend multimedia communication in IoV systems, buffer-aware QoE/QoS and energy aware QoE/QoS optimization techniques have been proposed [4]. These techniques tend to apply Artificial Intelligence and Machine learning schemes to improvise the features like evaluating mobility speed and direction, strength of network and works better up to a certain extent.

The notion of connected vehicles has been a potential innovation in the field of transportation but there is always a risk of cyber-attacks as in any other smart technology. These risks include DoS (Denial of Service), Hijacking, Man in the Middle Attacks (MIMA), etc. Protection against these threats and assurance of security from the attackers have become crucial for the progress in IoV to ensure the safety of the users [5]. The security threats come into the picture by focusing mainly on four main factors which are data, network vulnerabilities, vehicle security, and service platform security. Security aspects of network vulnerabilities include risks of utilizing Wi-Fi, cellular network, satellite network, wireless LAN, LTE-V2X/ DSRC, etc. This paper focuses on the data risks of the users by implementing federated learning to the data part to reduce privacy and security concerns in exchanging sensitive data with each other. The data risks include the questions about what type of data to be collected, how much to collect, and how it can be securely transferred and utilized without destroying the utility. Typically, the security requirements include data classification, transmission security, storage security, and privacy protection, keeping in mind confidentiality, integrity, and availability of the data. The spread of sensitive information should be discovered and such vehicles must be rescinded from the network. By performing such actions, trust can be maintained and user's and also vehicle's information will be protected and trust can be maintained.

At present, many trust models work by assessing nodes or data at application layer. Therefore, existing mechanisms could be categorized into cryptography-based elucidation and trust models. While the prior class alleviates risks, it is too slow and unreliable for everyday use and can be decoded [6]. The subsequent trust solution can assure similar level of security

without network delays and is reliable than the preceding one. In the context of connected vehicles, trust can be described as the belief that one vehicle puts in another regarding the information that is shared, to be genuine and authentic. Trust models are grouped based on data being centralized or node or even combined in turn depending on the rescission targets. Several metrics are taken into consideration while working with such models like analyzing messages, recommendation exchanges, assessing interactions, etc. Similar to the ones mentioned above, several protocols and standards have been set up to overcome the cyber risks and enhance the privacy and security of the users. Despite various measures being taken up, still attacks are continuous and there is always a risk of cyber-attacks.

Federated learning is a machine learning method that prepares a learning algorithm across different decentralized edge gadgets or servers holding nearby information tests, without trading them. This approach remains in contrast to conventional concentrated machine learning methods where all the nearby datasets are transferred to one server, as well as to additional classical decentralized approaches which frequently assume that neighborhood information tests are indistinguishably circulated. Federated learning empowers numerous entertainers to fabricate a typical, vigorous machine learning model without sharing information, in this manner permitting to resolve basic issues, for example, information protection, information security, information access privileges and admittance to heterogeneous information. Its applications are spread over various businesses including safeguard, media communications, IoT, and pharmaceutics. A significant open inquiry right now is the means by which sub-par models learned through federated information are comparative with the ones where the information are pooled. One more open inquiry concerns the dependability of the edge gadgets and the effect of vindictive entertainers on the learned model. Therefore, federated learning is proposed to mitigate risks and ascertain hacks instead of simple encryption, and other privacy-enhancing mechanisms.

Federated learning is the mechanism through which the training is directly deployed to local machines instead of collecting users' data and risking their privacy. The model learns from training instances of local users' data and updates the model to the cloud. The updated model is then deployed to other devices and trained on other users’ data and this process continues. Such data will not disturb users' privacy and is promising as no traces of users' data will be found on the trained model and can be reliable. This paper focuses on federated learning to detect the dissemination of information or any kind of vindictive behaviour possessed by the vehicles in the network. Federated learning is applicable to the proposed IoV environment as

in IoV ecosystem, and much of the computation must be done in the local side (across the IoV). Also, certain degree of learning is to be performed at the central level by the base station (global learning model). Hence, the federated learning model fits into the proposed framework.

2. Related Works

In IoV, the trust model's main goal is to be advantageous to provide an environment where data can be generated among network components in a stable and secure environment. Additionally, the trust mechanism ensures that each participating hub data is trusted. However, due to the unpredictability, exceptionally considering the IoV's mobile nature and trust promptly, the timeframe is quite challenging.

Node-centric trust models:

Node-Centric Trust (NCT) models evaluate the dependability of the message-sending vehicles intending to remove false nodes from the system. These trust models rely heavily on their neighbors, whose main duty is to maintain the popularity of the message carrier to supply opinions to the Message Evaluator node (MEval) [7]. For example, Yang developed an innovative NCT, specifically the "Trust and Reputation Management Structure," where the dependability of the message sender was analyzed using a comparability mining approach. MEval evaluates the similarity between messages when they are distributed throughout the network based on Euclidean distances and the reputation weights of the associated nodes. The scope of this strategy is constrained because the MEval analyses trust locally. However, few researchers have modified a model of economic incentives to keep dishonest nodes out of the network. According to this approach, a specific credit value is applied to each node inside the organization. The network node's behavior determines whether the credit increases or decreases; in other words, credits rise when a node behaves well. In the occurrence of an attack, the participating hub's credit is reduced. If the hub's credit is zero, MEval identifies it as harmful and eliminates it from the network. This trust model's central problem is that it does not distinguish between direct or indirect trust. A trust model based on suggestions was put forth to control local network attackers. In the suggested trust model, trust is calculated entirely decentralized using the weighted-total method [8]. Additionally, this trust model gives the evaluator node to record trust using both direct and indirect trust mechanisms. But, this trust model's major downside is its tendency to calculate trust using a weighted total, which might lead to a one-sided estimation of trust if the evaluator node is accompanied by more hostile nodes than otherwise, affecting the security of the network.

Data-centric trust models:

Instead of boycotting vehicles (IDs), Data-Centric Trust (DCT) models typically focus on sorting through harmful messages because the latter action may result in the unintended situation of a network interruption [9]. This job will be done by either removing messages from fake IDs or by reviewing the transferred messages themselves to make sure they are not encrypted. A data-centric trust model was also developed where sophisticated and predictable techniques were combinedly given. They calculate the closeness among messages representing the same event in the first. They then select through the various minority of messages under the assumption that the majority are genuine messages. However, the predictable methodology is dependent on the positioning of the vehicles and the measurement of the signal intensity. By analyzing the two characteristics, harmful vehicles and their messages can be recognized. In simple situations, it is slow and cannot progress as expected. A huge quantity of transporting vehicles is also needed to carry out this arrangement**.** Few researchers have also suggested a data-centric trust model termed Enhanced Distributed Trust Computing Protocol before the evaluation of direct associations among vehicles and with really no negotiated suggestions [10]. Each vehicle in this setup checks the accuracy of the event set off messages sent by its neighbors. A trust value will subsequently be assigned to the message source based on its reliability after the check-in of this proposal, which is assumed to be made only by nodes inside a similar event zone. The authors of this study also suggested a level-based message spreading technique to distinguish between modified messages and crafted events. But, to do this task, multiple vehicles must be present inside the event zone.

Combined Trust Models:

Together "entity" and "information" are properly considered in this particular classification of the trust models to evaluate reliance on the node and its shared information. As a result, combined trust balances the positive and negative aspects of NCT and DCT [10]. Furthermore, many standardized measures that evaluate the reliability of both the information and the node have been suggested.

Other studies have suggested a computed based trust calculation technique, where MEval directly monitors the events taking place inside the network, to distinguish nodes communicating corrupted data inside the network. The nearby vehicles inform MEval of the event's details. Through calculated judgment and strategic trust capabilities, MEval classifies the source node behaviour in perspective of the provided data as real or malicious. Although

this strategy is effective in detecting unethical vehicles, it can spread harmful material throughout the network. The trust calculation can be affected if MEval is surrounded by unethical nodes because of its tendency to evaluate trust in context of weighted voting. Researchers have essentially proposed a productive assault safe combined trust model, where MEval evaluates both node and information driven trust in order to decide trust on the obtained data. Based on Bayesian Inference, where MEval is based on data obtained from several neighbours, the information reliability is evaluated [11]. But at the other side, MEval coordinates Recommendation Trust (RT) and Functional Trust (FT) to analyze node driven reliability. While FT maintains that the speaking node behaves correctly while conversing with MEval, RT claims that a certain level of confidence must be maintained before the node can be depended upon. The information sparsity that is essential to IoV is not taken into account in this plan**.** In IoV, various trust models have been put out, providing the formation of trusted information in the network. In the event that a node is declared as reliable at a lower tier, node reliability is calculated at the transport layer but information reliability is only evaluated at the application layer [12].

3. Proposed mechanism

An impetus based Federated Learning (FL) for IoV has been proposed. The system model consists of a Base Station (BS) with capacity to store and transmit information in the smart transportation ecosystem. The presence of heterogeneous data makes it useful to have a learning mechanism in place for the participating entities that provide different types of functionalities.

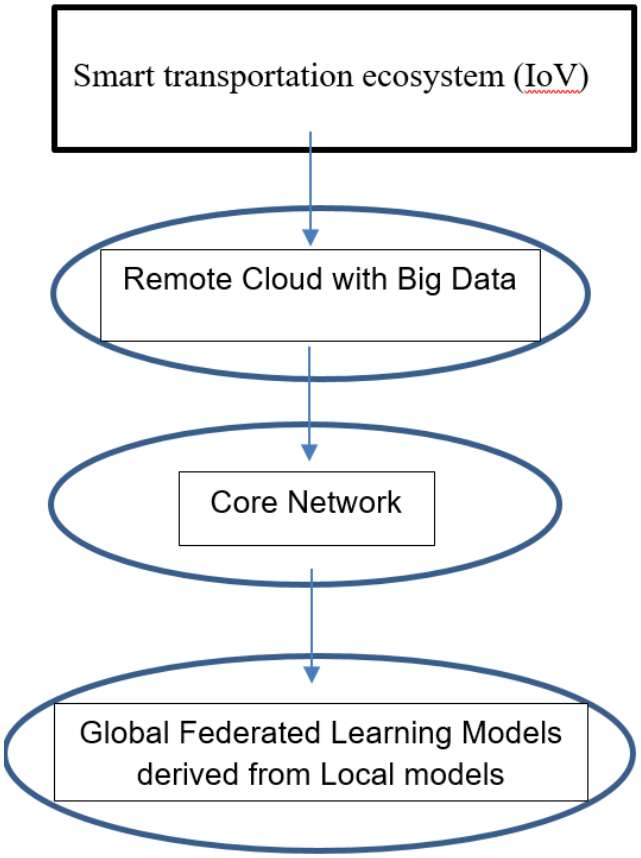

Figure 1. Federated learning for IoV

Suitable Design Considerations:

1. The IoV entities which participated in FL ecosystem must get a prize within each BS for one global loop that learn to conserve maximum energy in minimum amount of learning time.

2. The group of IoV entities are resource constrained with respect to capacity of computation training data size and transmission channel conditions.

3. To tackle the difficulty of synchronization of both IoV and data, the accuracy of global and local data models are different.

4. For selecting an IoV in BS for FL, the training cost should be considered rather than the cost of improving accuracy.

5. Now, the best candidate among a group of IoV is selected for federation learning by applying bounded rationality principle. As per this principle, obtaining a satisfactory response rather than obtaining an optimal response during decision making process is attempted.

6. The core network consists of the server with co-ordinates for the training of the global learning model at the BS. The base station receives signals from the various participating IoV as illustrated below.

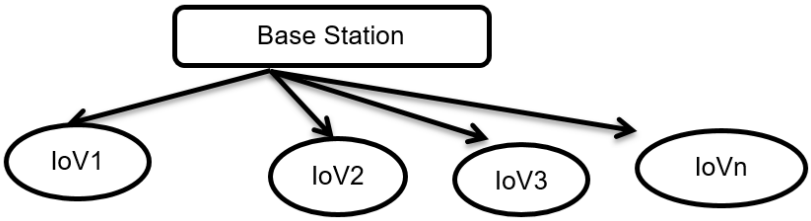

Figure 2. Illustration of the operation of Core Network

Algorithm:

Step1: At the onset, each IoV entity gives its best signal /response to the BS to maximise its reward (local condition).

Step 2: The BS evaluates the entire signal and updates the global learning model based on its satisfactory reward.

Step3: The BS sends a reward rate to each of the participating entities as per the maximum rate of satisfaction.

Step 4: Given the maximum satisfaction reward to the IoVs, each IoV updates its local learning model, thus trying to maximise its local utility.

Steps to derive the global federated model from local models:

Step 1: Generate a contribution matrix from local explanations of each IoV, by using model specific objectives.

Step 2: Use recursive partitioning technique to send the contribution matrix from each participating IoV to the global federated learning model present in the base station.

Step 3: The global federated learning model returns an interpretation tree which is comprehensible by human users.

Step 4: Human users' cognition helps in classification of user behaviour as malicious or legal action.

Necessary steps of each iteration of the federated learning global model:

1. The learning nodes in each participating IoV train their local model and then send the local parameters to the server.

2. The server at the base station determines a weighted averaging of the model and sends the global parameters back to the learning nodes in the participating IoVs.

3. Now, each IoV finetunes their learning parameter before initiating the next iteration. The learning parameters include factors on which a malicious user is defined. In few instances, there may be false positives and false negatives which have to be eliminated by the local learning models by adjusting their learning factors.

Bounded rationality principle refers to a type of decision making process by a human user where the objective is to satisfy a result rather than optimize the result. It does not aim to obtain a best result but settles for a solution which provides highest level of satisfaction. The reason why the bounded rationality principle is suitable in the proposed approach is that, in federated learning, both the global and local learning models have a trade-off during training process; so, to balance this trade-off, bounded rationality principle holds the equilibrium stage. It helps in reaching a satisfying condition rather than a best solution. The main advantage of applying bounded rationality principle to reach an equilibrium state is that it avoids the problem of winner's curse. The winner's curse is the most general problem faced by the decision makers during all the optimization problems. The winner's curse states that in order to reach the optimal solution, the decision maker overpays (or) overestimates the assets. During federated learning, if the base station gives more reward to an IoV, then the cost of global learning will increase. To avoid this, bounded rationality can restrict the degree of optimality by giving a satisfactory reward from the base station to the IoV.

4. Results

The main challenge in implementing the algorithm proposed is the procurement of input data. The data in IoV environment is highly unstructured and discrete data due to loss in internet connectivity during data transmission among the various sensors involved in the environment. It was found difficult to get real time dataset, therefore a generated dataset form of the popular

simulators used by various researchers in modelling IoV ecosystem has been used. In federated learning, the data models need large amount of data for solving classification clustering and prediction problems. Apache Spark has been used as the big data analytics framework.

The vehicular versatility dataset is fundamentally founded on the data made accessible by the Travel and Activity PAtterns Simulation (TAPAS) Cologne project. TAPAS Cologne is an initiative of the Institute of Transportation Systems at the German Aerospace Center, pointed toward replicating, with the most elevated level of authenticity conceivable vehicle traffic in the greater metropolitan region of the city of Cologne, in Germany. The deducted synthetic trace of the traffic of car travels considered in the city of Cologne includes an area of 400 square kilometres for a duration of 1 day which consists of nearly 700 trips. With that in mind, different state-of-workmanship, data sources and simulation devices are united. So to cover every one of the particular viewpoints expected for a legitimate characterization of vehicular traffic:

• The road design of the Cologne metropolitan region is acquired from the OpenStreetMap (OSM) database;

• The minuscule versatility of vehicles is simulated with the Simulation of Urban MObility (SUMO) software;

• The traffic request information on the naturally visible traffic streams across the Cologne metropolitan region (i.e., the O/D matrix) is inferred through the TAPAS philosophy;

• The traffic task of the vehicular streams portrayed by the TAPAS Cologne O/D matrix over the street geography is performed through Gawron's dynamic client task calculation.

The platform used for conducting simulations is Eclipse SUMO, which is an open source, highly portable, microscopic and continuous multi-modal traffic simulation package which was made to face data which originates from large networks. The metrics used by the federated learning algorithm are precision and recall, based on which the F1 score is computed to determine the performance results

Table 1. Comparative Analysis of Popular methods

S. No.	Technique	F1-Score
1	Support Vector Machine	0.73
2	Random Forest	0.82
3	Decision Tree	0.85
4	Proposed Federated Learning model	0.91

As shown in Table 1, the technique of Support Vector Machine for classification of malicious behaviour has F-1 score based on factors of precision and recall at 73%. It can be improved further by application of better methods like Random Forest and Decision Tree algorithms which have a F1-score of 82% and 85% respectively. But the most promising method is the proposed mechanism using federated learning which shows F1 score of 91%. In figure 2, the plot shows the performance against accuracy. On x-axis, the percentage increase in accuracy is used and on y-axis, the percentage increase in malicious behaviour of detection score is shown, and the highest growth in the graph is obtained by the proposed federated learning based detection method.

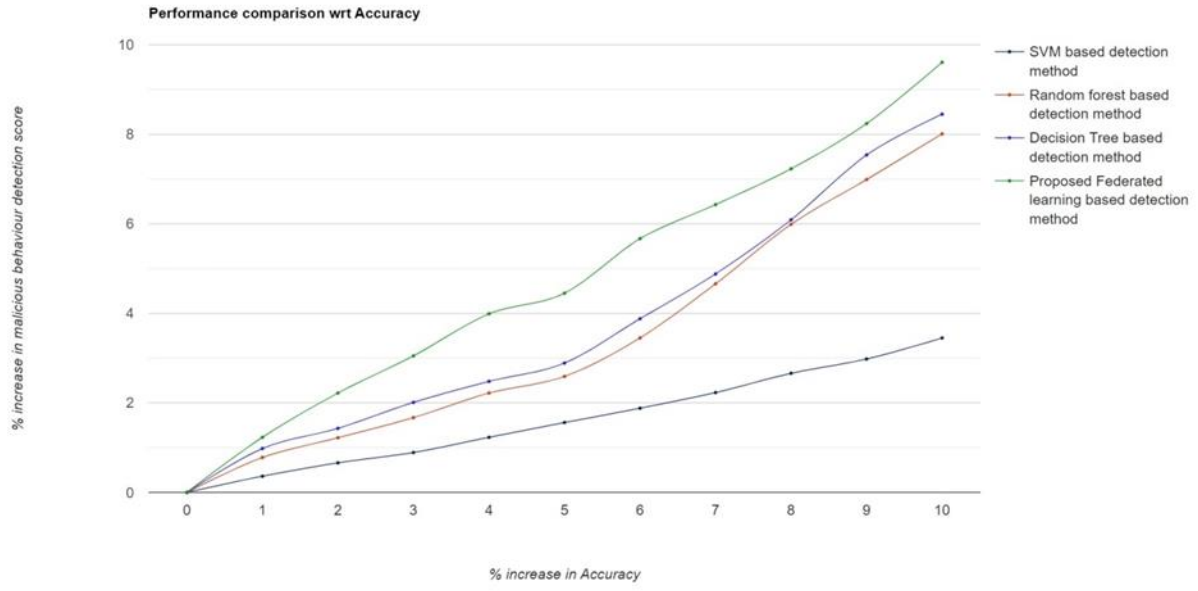

Figure 3. Performance comparision with respect to accuracy of popular existing methods.

5. Future Directions

In future, provisions to face challenges like the effect of autonomous vehicles in an IoV ecosystem as well as handling heterogeneous data sources, and synchronizing them for better degree of classification and prediction would be developed. Compatibility issue is another test confronting the smooth operation of the IoV. The communications between vehicles, particularly V2V, are being tested. The V2V innovation in a vehicle ought to be compatible, preceding the trade of data between the vehicles. In the event that the V2V innovation in a vehicle isn't compatible with another V2V innovation in another vehicle, no communication between the vehicles would exist. Consequently, these vehicles can't communicate inside the IoV climate. The data generated from the vehicles and moved to focal handling framework for data examination, can only with significant effort, give uniform choice to the vehicles inside the IoV climate. The data generated from a specific vehicle get a choice not the same as the data generated from vehicles with various V2V innovations. Therefore, having uniform choice is limited exclusively to vehicles with compatible V2V advancements.

6. Conclusion

Detecting malicious behaviour in IoV environment is difficult because the learning architecture of the subsystems may not be the same, since the software used by the participating vehicles may not be the same. This paper is a step towards detecting suspicious behaviour by any user involved in IoV ecosystem. In the paper, the learning models, either Global or Local learning models, need to be supplied with input data to train them for detection of malicious behaviour. Yet another challenge is that the definition of malicious behaviour needs to be standardized so that the vehicles participating in the IoV architecture operate in a uniform manner, thus providing stability for the federated learning model.

7. References

[1] Sahraoui, Yesin, et al. "DeepDist: A deep-learning-based IoV framework for real-time objects and distance violation detection." IEEE Internet of Things Magazine 3.3 (2020): 30-34.

[2] Alatabani, Lina Elmoiz, Elmustafa Sayed Ali, and Rashid A. Saeed. "Deep learning approaches for IoV applications and services." Intelligent Technologies for Internet of Vehicles. Cham: Springer International Publishing, 2021. 253-291.

[3] Sassi, M. Saifeddine Hadj, and Lamia Chaari Fourati. "Investigation on deep learning methods for privacy and security challenges of cognitive IoV." 2020 International Wireless Communications and Mobile Computing (IWCMC). IEEE, 2020.

[4] Yaqoob, Shumayla, et al. "Deep Learning based Anomaly detection for Fog_assisted IoVs Network." IEEE Access (2023).

[5] Zhao, Peng-Cheng, et al. "CCP-federated deep learning based on user trust chain in social IoV." Wireless Networks (2022): 1-12.

[6] Kumar, Randhir, et al. "P2SF-IoV: A privacy-preservation-based secured framework for Internet of Vehicles." IEEE Transactions on Intelligent Transportation Systems 23.11 (2021): 22571-22582.

[7] Mahmood, Adnan, et al. "Trust on wheels: Towards secure and resource efficient IoV networks." Computing 104.6 (2022): 1337-1358.

[8] Sharma, Richa, Teek Parval Sharma, and Ajay Kumar Sharma. "Trust assessment-based stable and attack resistant grouping strategy for data dissemination in IoV." International Journal of Sensor Networks 40.3 (2022): 160-174.

[9] Bhardwaj, Indu, Sibaram Khara, and Priestly Shan. "A Framework to Systematically Analyse the Trustworthiness of Nodes for Securing IoV Interactions." Scalable Computing: Practice and Experience 21.3 (2020): 451-462.

[10] Chouhan, Piyush, and Swapnil Jain. "Trusted Multipath Routing for Internet of Vehicles against DDoS Assault Using Brink Controller in Road Awareness (TMRBC-IOV)." Autonomous Vehicles Volume 1: Using Machine Intelligence (2022): 39-60.

[11] Sassi, M. Saifeddine Hadj, and Lamia Chaari Fourati. "Investigation on deep learning methods for privacy and security challenges of cognitive IoV." 2020 International Wireless Communications and Mobile Computing (IWCMC). IEEE, 2020.

[12] Ayaz, Ferheen, et al. "Blockchain-enabled security and privacy for Internet-of-Vehicles." Internet of Vehicles and its Applications in Autonomous Driving (2021): 123-148.